OnTek

PROTEJA SU EMPRESA ONLINE ANTE EL RELLENO DE CREDENCIALES

ANTICÍPESE A LAS AMENAZAS CON UNA TECNOLOGÍA AVANZADA DE GESTIÓN DE BOTS

El coste total asociado al relleno de credenciales, incluidos las pérdidas por fraude, la seguridad operacional, el tiempo de inactividad de las aplicaciones y el abandono de clientes, puede oscilar entre 6 y 54 millones de dólares al año.

Fuente: The Cost of Credential Stuffing, Ponemon Institute, 2017

Cuando alguien inicia sesión en su sitio web, ¿cómo distingue entre el uso legítimo y el relleno de credenciales? No saber si un inicio de sesión proviene de un usuario real o de un programa de software que lo imita hace que su empresa sea vulnerable al fraude.

Con la proliferación de aplicaciones online, la mayoría de los usuarios no siguen unas buenas prácticas de seguridad en Internet, ya que reutilizan las mismas credenciales de inicio de sesión en distintas cuentas. Esto convierte a cualquier empresa online que tenga una página de inicio de sesión en un posible objetivo para el relleno de credenciales, tanto si ha sufrido una filtración de datos como si no.

Cuanto mayor sea el valor de la transacción, mayor es el riesgo. Un estafador puede adquirir artículos en una tienda online, contratar préstamos bancarios en una institución financiera o robar la información médica de un sitio perteneciente al sector sanitario. El relleno de credenciales puede perjudicar a su negocio, sus clientes y su marca, y, dada su naturaleza furtiva, necesita herramientas especializadas para detectarlo y protegerse contra él.

Conocer las amenazas de relleno de credenciales, su creciente sofisticación y las mejores formas de abordarlas puede ayudarle a proteger su empresa.

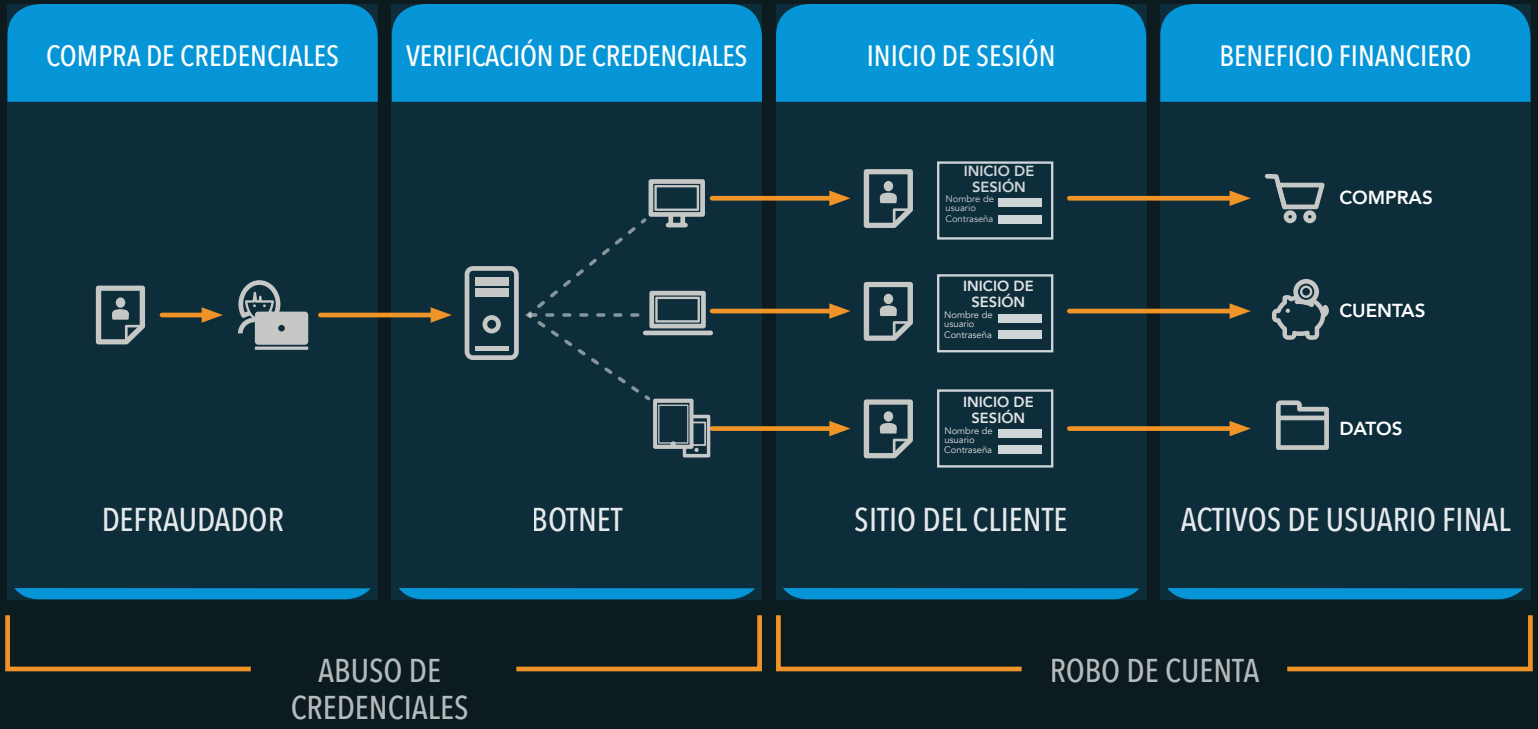
INCLUSO LAS EMPRESAS MÁS SEGURAS ESTÁN EXPUESTAS

Las estimaciones recientes del sector indican que son miles de millones las credenciales (nombres de usuario, contraseñas y direcciones de correo electrónico) robadas que están en circulación en la actualidad. Según un informe de 2017 de Frost & Sullivan, "para los atacantes, es solo una cuestión de cifras: una tasa de éxito del 1 % tras mil millones de intentos dará como resultado 10 millones de filtraciones".

Las credenciales de cliente a menudo son pirateadas como consecuencia de intrusiones en otros sitios. A continuación, esta información se vende en el mercado negro como conjuntos de datos individuales o múltiples, a precios que van desde menos de un dólar para el contenido de primera calidad a miles de dólares en el caso de cuentas bancarias con saldos elevados. Un estudio de la Comisión Federal de Comercio (FTC) de EE. UU. ha revelado que los hackers solo tardan 9 minutos en empezar a acceder a las credenciales robadas, una vez publicadas.

La red y los datos se pueden proteger de forma segura, pero su empresa seguirá estando expuesta al fraude si no puede detectar y detener el relleno de credenciales antes de que se encuentre una combinación correcta. En una encuesta realizada por Ponemon Institute recientemente, más de la mitad de los encuestados señalaron el relleno de credenciales como un importante reto en materia de seguridad para sus empresas. Además, casi el 70 % de los encuestados afirmaron no tener la sensación o no estar seguros de si sus empresas tenían una visibilidad adecuada de estos ataques.

ABUSO DE CREDENCIALES



EL RELLENO DE CREDENCIALES DERIVA EN EL ROBO DE CUENTAS

El relleno de credenciales comienza cuando un atacante intenta verificar información de usuario robada en los sistemas de inicio de sesión de sus sitios web. Una vez que se confirma un subconjunto de inicios de sesión válidos, el atacante puede revender la lista a otro estafador, o bien realizar directamente el robo de las cuentas online, extrayendo de estas todo aquello que sea rentable.

A diferencia de otros ataques a aplicaciones web, como la inyección SQL, las solicitudes de inicio de sesión derivadas del relleno de credenciales no tienen patrones que se puedan identificar y bloquear fácilmente. Las verificaciones de credenciales son solicitudes válidas (la información de inicio de sesión es legítima, pero no la entidad que intenta autenticarse en una cuenta), por lo que son casi imposibles de detectar.

Afortunadamente, el proceso de verificación de credenciales robadas (o relleno de credenciales) no se suele realizar manualmente. Esta es su oportunidad de intervenir. La validación suele estar automatizada, lo que hace que el relleno de credenciales sea un problema de bots desde el principio.

CÉNTRESE EN EL PROBLEMA DE LOS BOTS

Los bots generan entre el 30 y el 70 % del total de tráfico de los sitios web actuales.

Fuente: 10 principales consideraciones para la gestión de bots

Su capacidad para detener los ataques de relleno de credenciales depende de lo preparado que esté para detectar y mitigar bots. Poner fin a esta actividad antes de que se produzca el robo de cuentas le permite:

- Identificar el uso indebido con más facilidad, ya que las solicitudes de inicio de sesión generadas por bots son más fáciles de detectar que los robos de cuenta realizados por humanos.
- Reducir la incidencia de intentos de robo de cuentas, al reducir el número de credenciales validadas disponibles para los estafadores.
- Hacer que su sitio web sea menos atractivo para los estafadores, que suelen centrarse en los objetivos menos protegidos.

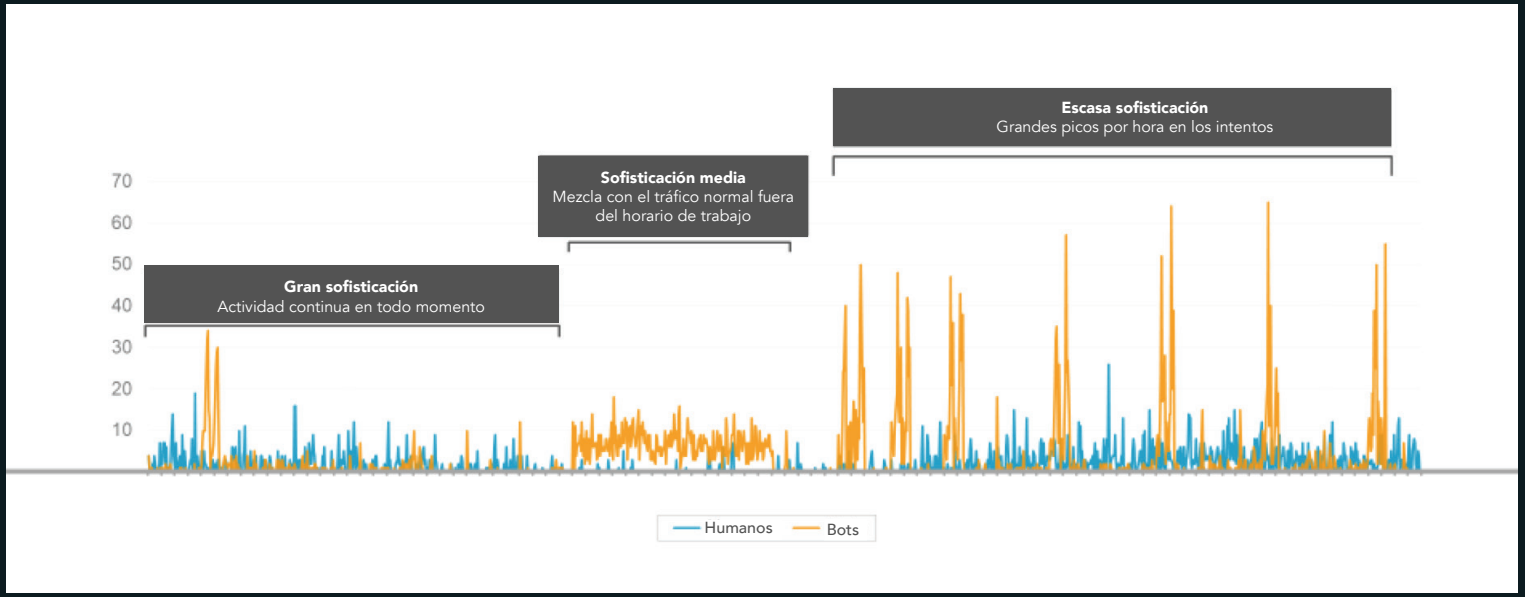
En pocas palabras, un bot es un software que se ejecuta en un servidor conectado a Internet que interactúa con otras entidades online, tales como su sitio web. Varios bots enlazados forman una red conocida como botnet, que puede hacer rápidamente lo que, de otra forma, sería un proceso laborioso, como es la introducción de cientos, miles o decenas de miles de credenciales de inicio de sesión. Y, detrás de este software, está el operador del bot: la persona u organización que creó el script.

LAS AMENAZAS EVOLUCIONAN RÁPIDO

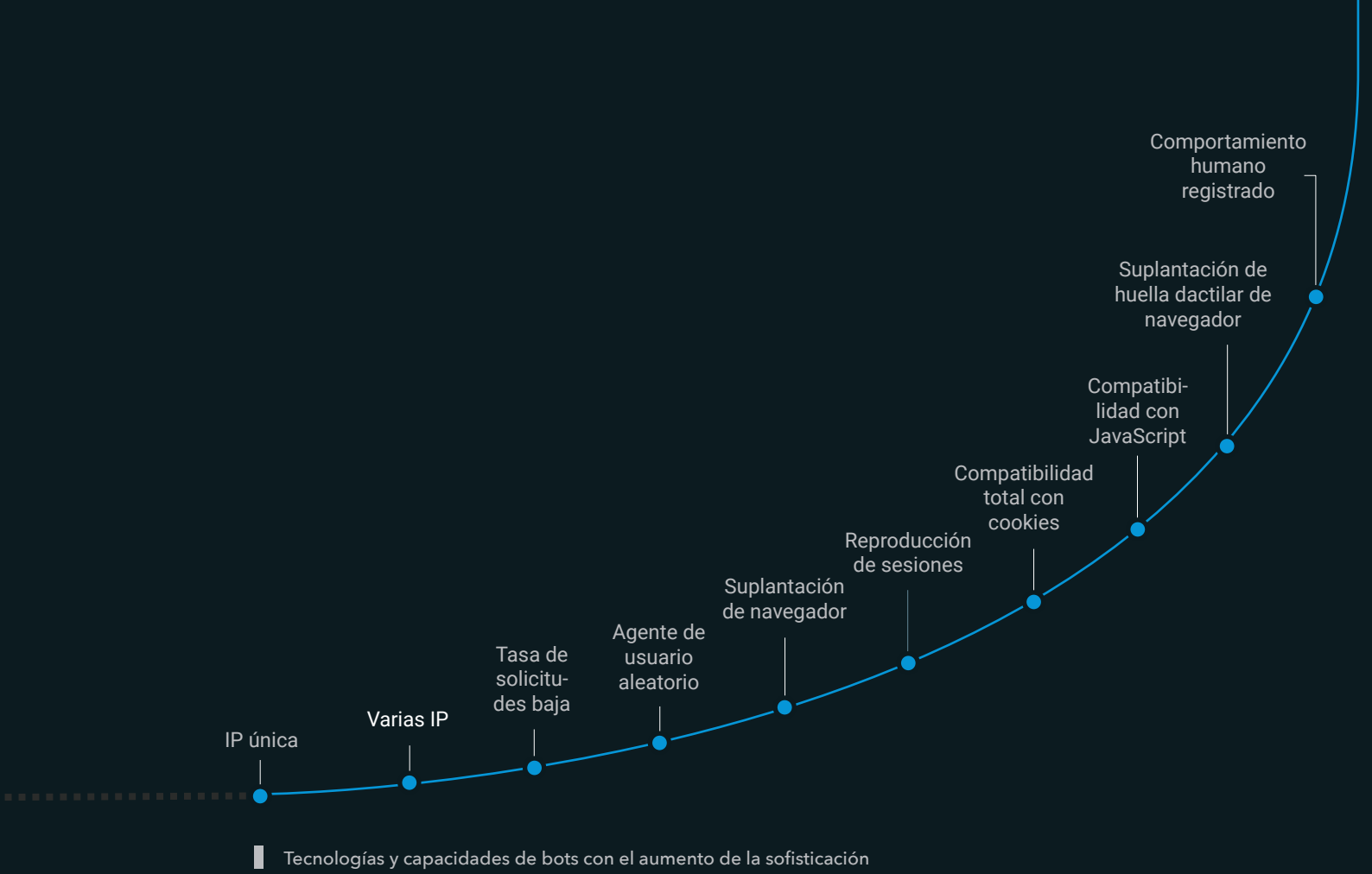
Una vez que se detecta un bot, su respuesta puede afectar a la viabilidad de una solución. Si un operador observa que ha encontrado el bot, intentará averiguar cómo lo ha hecho y actualizará el software para evitar la detección. Con oportunidades de robo de cuentas rentables, el relleno de credenciales atrae a algunos de los operadores de bots más sofisticados y presenta una tasa más elevada de evolución de bots.

Existe una amplia gama de bots, que va desde scripts simples a herramientas de automatización complejas, y que cambia continuamente a lo largo del tiempo. Para evaluar la sofisticación de una amenaza de relleno de credenciales, puede medir el patrón del tráfico de inicio de sesión o las tecnologías y capacidades utilizadas.

Si solo atiende a los picos de inicio de sesión, puede que alguna actividad mucho más seria pase desapercibida. La mayoría de los sitios web interactúan con una variedad de amenazas cada día: desde una clara automatización hasta el comportamiento de bots más evasivo. Un ataque de fuerza bruta procedente de unas cuantas direcciones IP requiere una estrategia diferente que para un bot con un comportamiento humano registrado y con solicitudes escasas y esporádicas por dirección IP.

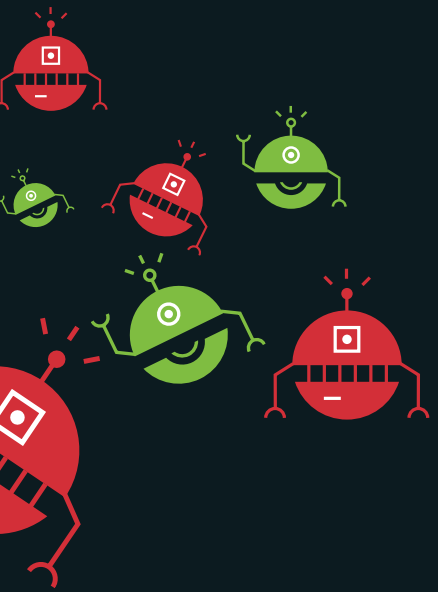


Sofisticación de bots por patrón de tráfico con distintos niveles detectados en un periodo de 24 horas



Tecnologías y capacidades de bots con el aumento de la sofisticación

HAGA FRENTE A LA CRECIENTE SOFISTICACIÓN DE LOS BOTS

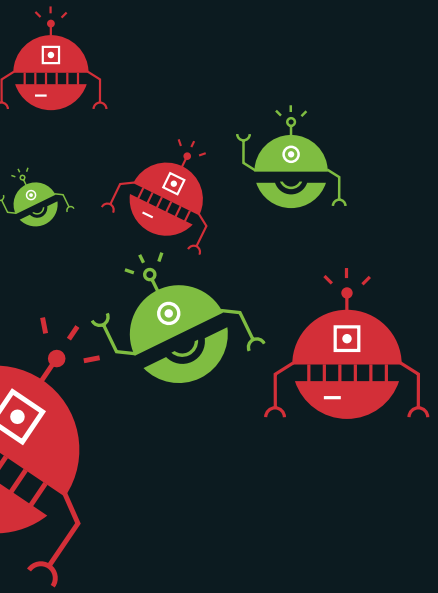


Conforme mejoran las tecnologías de detección, también lo hacen las técnicas de evasión disponibles para los operadores de bots. Una estrategia eficaz de gestión de bots no es estática, y debe tener en cuenta el panorama actual y futuro de los bots para anticiparse a las amenazas. Echemos un vistazo a cada amenaza según su nivel de sofisticación para determinar qué enfoque de gestión de bots es el adecuado para su negocio.

ESCASA SOFISTICACIÓN

- Genera grandes picos de solicitudes de inicio de sesión desde una dirección IP única o varias direcciones, llegando a alcanzar varias veces picos superiores al tráfico humano legítimo.
- Utiliza generadores de agentes de usuario aleatorios, suplantación de navegador y reproducción de sesiones.
- Activa alertas de herramientas de gestión de tráfico y de seguridad sin capacidades específicas de detección de bots.

La forma más simple de relleno de credenciales comienza con un bot que hace intentos de inicio de sesión repetidamente. El aumento de las solicitudes procedentes de una única dirección IP es fácil de detectar y bloquear con herramientas estándar de gestión del tráfico. Ojalá todo quedara en eso.

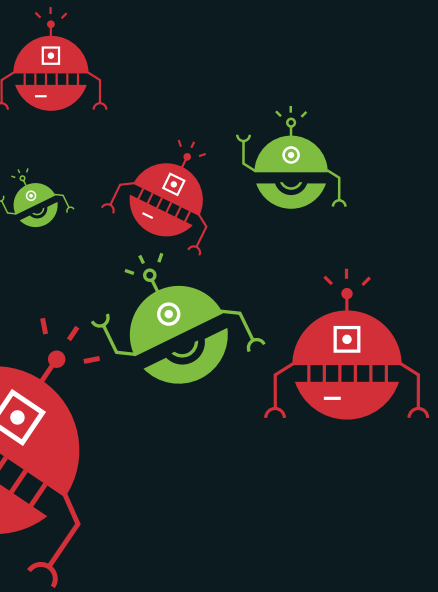


Lo siguiente es que los operadores pasan a botnets con varias direcciones IP, que van desde unas pocas hasta cientos de ellas, con un volumen de solicitudes de inicio de sesión procedentes de cada dirección IP inferior con respecto a antes. El bloqueo sigue siendo posible, pero empieza a convertirse en un proceso tedioso debido al mayor número de direcciones IP. La limitación de velocidad puede bloquear automáticamente las direcciones IP individuales que superen el umbral máximo de solicitudes dentro de un periodo de tiempo determinado. Sin embargo, es probable que los operadores reduzcan el ritmo de solicitudes para volver a pasar desapercibidos.

Para imitar mejor el tráfico generado por un navegador, los operadores actualizan los programas para falsificar diversos campos del encabezado de solicitud, como el agente de usuario. Un firewall de aplicaciones web (WAF) o herramientas propias pueden detener a estos bots, aún simples, mediante el uso de reglas personalizadas para identificar y bloquear determinados campos del encabezado. Sin embargo, estas soluciones pasan rápidamente a ser inviables a medida que las amenazas evolucionan.

Por ejemplo, si se detecta una botnet que envía solicitudes de inicio de sesión desde un agente de usuario común, puede crear reglas que lo identifiquen y le impidan el paso, pero el operador puede cambiar el agente de usuario una vez bloqueado, y usted deberá volver a identificarlo. Sin una solución de gestión de bots especializada, llegará a un punto, normalmente con la limitación de velocidad, en el que simplemente no tendrá la experiencia o los recursos para atajarlos.

HAGA FRENTE A LA CRECIENTE SOFISTICACIÓN DE LOS BOTS

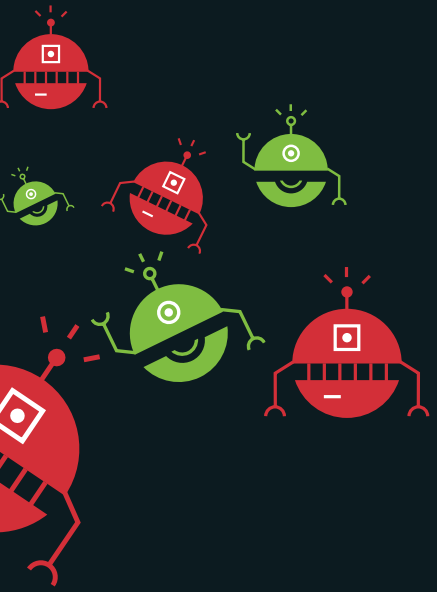


SOFISTICACIÓN MEDIA

- Genera una concentración de solicitudes que salta a la vista y que suele tener lugar durante la noche, pero con un nivel similar al del tráfico legítimo.
- Utiliza JavaScript y es totalmente compatible con cookies.
- Requiere un partner de tecnología de gestión de bots o una solución para detectarlos y evitarlos.

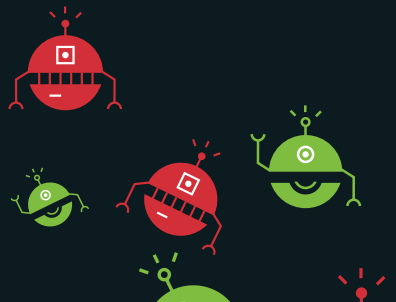
Las IP dinámicas (con cientos o miles de bots rotando por distintas direcciones IP) pueden reducir la eficacia de los controles de frecuencia. Inyectar un desafío de JavaScript suele ser el primer paso contra estos bots más difíciles de detectar, aunque sigan siendo relativamente simples. Pero JavaScript solo es un lenguaje de programación: el modo en que se utilice en los ataques automatizados determina su eficacia. Presentar un lenguaje a bots que no lo entiendan puede detener algunas amenazas, pero no las más sofisticadas.

Las herramientas más avanzadas son compatibles con JavaScript y pueden hacer frente a cualquier desafío. Recoja la huella dactilar del navegador, mediante la inyección de código JavaScript, no para presentar un desafío, sino para recopilar información identificativa. Con la huella dactilar del navegador, JavaScript recopila una gran variedad de características, tales como la resolución de pantalla, el tipo de navegador, plugins y fuentes. Estos detalles permiten identificar si el cliente utiliza un navegador automatizado o sin interfaz, así como la combinación única de características que revelan la fuente.

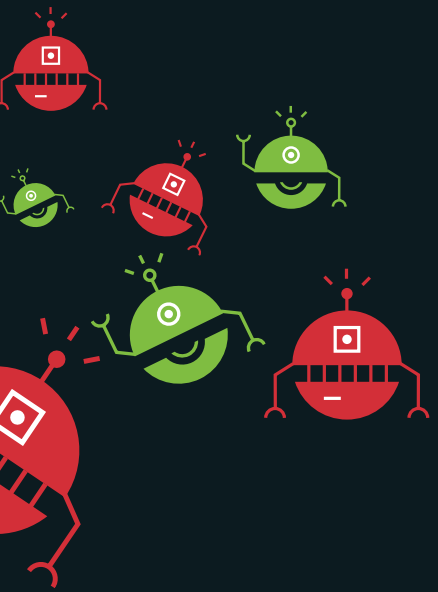


Una vez que tenga la huella dactilar, puede analizar las características de las anomalías; por ejemplo, si un navegador no admite un plugin específico. Puede utilizar dichos detalles para identificar y responder a la amenaza. También puede guardar la huella dactilar, de manera que si observa que hace lo mismo varias veces desde distintos dispositivos, por ejemplo, como parte de un ataque de relleno de credenciales, hay una mayor probabilidad de que sea un bot.

La huella dactilar del navegador es una de las tecnologías de detección más utilizadas, pero hoy en día existen herramientas populares de suplantación de huella dactilar del navegador que son fáciles de adquirir e implementar. Un operador de bots sofisticado o un estafador persistente puede eludir la huella dactilar del navegador, lo que la convierte en una barrera menos eficaz contra aquellos que se sienten atraídos por el negocio más lucrativo del relleno de credenciales.



HAGA FRENTE A LA CRECIENTE SOFISTICACIÓN DE LOS BOTS



GRAN SOFISTICACIÓN

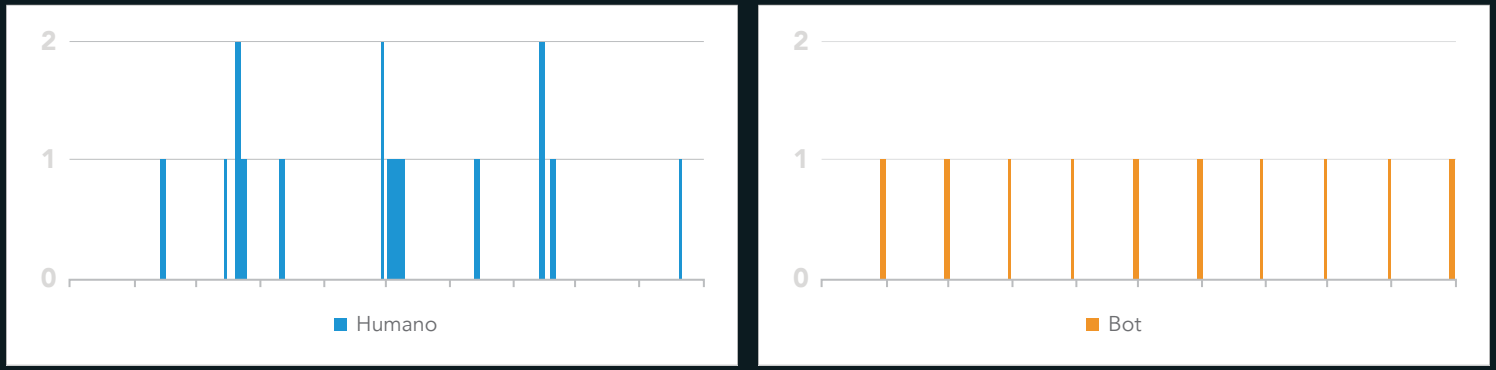
- Genera un nivel de actividad bajo y lento en un periodo de 24 horas desde una botnet distribuida masivamente, formada por miles o decenas de miles de bots que envían unas pocas solicitudes de inicio de sesión.
- Se sirve de direcciones IP desechables, suplantación de la huella dactilar del navegador y comportamiento humano registrado.
- Requiere técnicas de detección de bots especializadas, con análisis avanzados de anomalías en el comportamiento, para la detección.

Con el operador de bots menos sofisticado, la detección de anomalías en HTTP, los desafíos de JavaScript y la huella dactilar de navegador pueden ser suficientes para capturar la actividad. Sin embargo, es probable que un operador capaz de compilar una botnet distribuida masivamente consiga sortear estas estrategias. Gestionar esta amenaza altamente sofisticada implica una detección avanzada de bots que realice un seguimiento y analice las anomalías en el comportamiento.

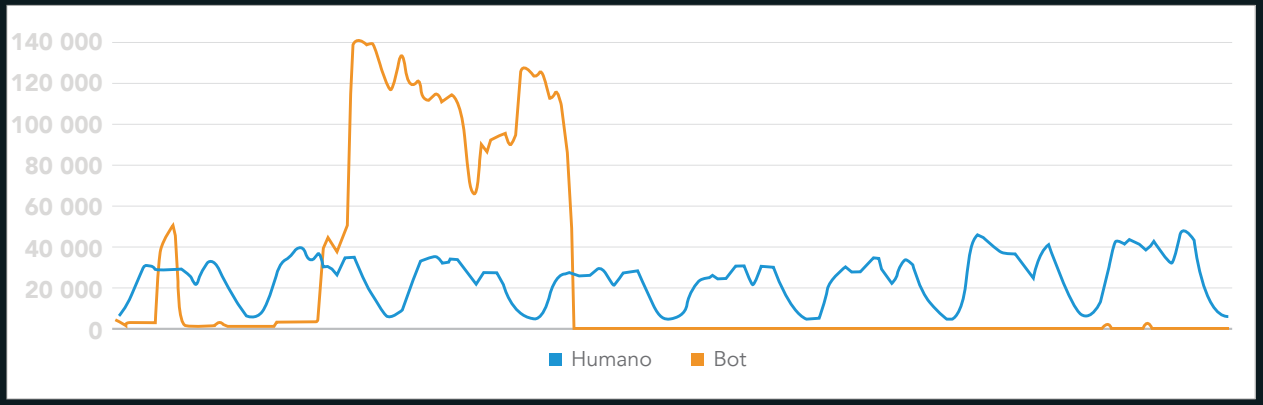
Las tecnologías de gestión de bots más recientes recopilan telemetría conductual para distinguir entre humanos y bots. Los análisis de anomalías en el comportamiento utilizan mediciones de los dispositivos de entrada de los usuarios, como las pulsaciones del teclado y los movimientos del ratón de un ordenador o acelerómetro, así como las lecturas del giroscopio de un teléfono móvil o tablet. Por ejemplo, un humano no puede mover físicamente un ratón en una línea recta perfecta, por lo que un ratón que interactúa con un sitio web de esa forma no puede estar accionado por un humano. Cuando se analiza conjuntamente, esta telemetría puede proporcionar una evaluación muy precisa de si un usuario es un humano o un bot.

Por supuesto, los operadores de bots pueden desarrollar telemetría aparentemente aleatoria para dificultar tal diferenciación. Además, cuando un conjunto de telemetría funciona, este se puede reproducir en distintos bots. La clave para ganar la partida a estas técnicas está en el análisis de telemetría.

Puesto que los bots más sofisticados pueden cambiar sus patrones para imitar mejor a los usuarios humanos, el éxito del análisis de anomalías en el comportamiento depende de su capacidad para identificar las pequeñas diferencias que determinan que la actividad no está realizada por un humano. Esto requiere un algoritmo de aprendizaje automático altamente optimizado para las variaciones entre el comportamiento humano y el de los bots.



El patrón de pulsaciones de teclas de un humano es esporádico y presenta intervalos irregulares entre cada pulsación en comparación con el patrón de un bot, que presenta intervalos regulares entre las distintas pulsaciones.



Número de intentos de inicio de sesión realizados por humanos y bots en una página de inicio de sesión de un importante retailer de moda durante un periodo de 8 días

CASO REAL

Después de un ataque de gran envergadura que llega a un pico de más de 131 000 solicitudes por hora, un importante retailer de moda empezó a bloquear el tráfico de bots con Akamai Bot Manager Premier. No solo redujo el tráfico de inicio de sesión de bots a una cantidad insignificante desde el punto de vista estadístico, sino que el nivel de tráfico de inicio de sesión por parte de humanos no cambió.

MINIMICE LOS FALSOS POSITIVOS

En lo que respecta al relleno de credenciales, reducir al máximo los falsos positivos es fundamental. Esto es especialmente cierto en el caso de la actividad de bots muy sofisticada que imita el comportamiento humano. Confundir un visitante humano con un bot puede bloquear el acceso de los usuarios a sus cuentas, provocar la insatisfacción de los clientes y ocasionar la pérdida de oportunidades de negocio.

Más del 70 % de los participantes en la encuesta realizada por Ponemon Institute coincidieron en que prevenir los ataques de relleno de credenciales es difícil, ya que las correcciones que limitan a los delincuentes pueden mermar la experiencia web de los usuarios legítimos.

La tecnología avanzada de aprendizaje automático y el análisis de anomalías en el comportamiento utilizados contra estas amenazas más sofisticadas proporcionan una mayor precisión. Cuanto más optimizado esté el algoritmo, más preciso será el análisis para minimizar el impacto en el rendimiento y el número de falsos positivos que pueden bloquear accidentalmente los inicios de sesión de los usuarios legítimos.

CALCULE EL IMPACTO FINANCIERO DEL RELLENO DE CREDENCIALES

El dinero que invierte en una solución de gestión de bots, ya sea propia o externa, básica o avanzada, debe ser proporcional al posible impacto financiero o en la marca que el relleno de credenciales puede tener en su negocio. Normalmente, su interés por esta área se alinea con el de los estafadores: cuanto más tenga usted que perder, más tienen ellos que ganar.

Para calcular el impacto, puede cuantificar el alcance de la actividad y vincularla a métricas conocidas como:

- **Dinero perdido a causa del fraude.** Valor medio de las transacciones fraudulentas mediante el empleo de credenciales robadas. Las métricas varían de un sector a otro, pero incluyen el valor medio de los pedidos o el saldo de las cuentas.
- **Costes de prevención del fraude.** Muchas organizaciones cuentan con soluciones antifraude que se tarifican según el número de consultas, por lo que reducir la incidencia de cuentas afectadas disminuye el coste de estas soluciones.
- **Costes de reparación.** La captura temprana de intentos de fraude reduce los gastos de reparación, ya que notificar a los clientes que deben cambiar sus credenciales cuesta menos que asignar un representante a una investigación de fraude.
- **Valor del cliente perdido.** Las transacciones fraudulentas pueden causar una pérdida de clientes, por lo que la mayoría de los sectores cuenta con una métrica para el valor del tiempo de vida de los clientes.

El equipo antifraude de una empresa del sector de los servicios financieros valoró la pérdida monetaria de 500 cuentas robadas por estafadores en 1 millón de dólares, lo que supone una media de 1923 dólares por cuenta.

He aquí un ejemplo.
Supuestos:

- 1 000 000 de intentos de inicio de sesión fraudulentos al mes
- 20 cuentas afectadas al mes
- 0,01 dólares por consulta de las soluciones antifraude
- 500 dólares de valor medio de la transacción fraudulenta
- 1000 dólares de costes de reparación por cuenta
- 2000 dólares de valor medio del tiempo de vida de los clientes
- Tasa de abandono del 20 % atribuida a las cuentas afectadas

1 000 000 × 0,01 dólares = 10 000 dólares de costes de prevención del fraude al mes

20 × 500 dólares = 10 000 dólares de costes por fraude al mes

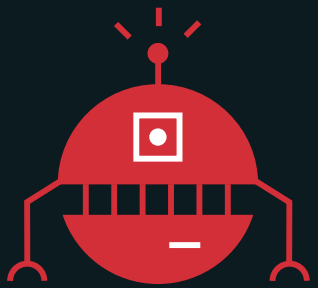
20 × 1000 dólares = 20 000 dólares de costes de reparación al mes

20 × 20 % × 2000 = 8000 dólares de pérdida de valor de clientes al mes

10 000 $ + 10 000 $ + 20 000 $ + 8000 $ = 48 000 dólares de valor total al mes

Si le añade el coste del posible tiempo de inactividad de las aplicaciones derivado de los picos de solicitudes de inicio de sesión, el impacto financiero podría ser aún mayor.

EL RELLENO DE CREDENCIALES SOLO ES UNO DE LOS MUCHOS PROBLEMAS RELACIONADOS CON BOTS



Para gestionar y mitigar correctamente las amenazas de bots más recientes, como el relleno de credenciales, necesita una solución de bots específica y moderna con las detecciones más recientes y avanzadas. Hoy en día, esto equivale al análisis de anomalías en el comportamiento y los algoritmos de aprendizaje automático con el número mínimo posible de falsos positivos.

Sin embargo, probablemente los problemas de bots vayan más allá del relleno de credenciales para incluir el scraping web, la agregación de contenido y la buena gestión de bots, por citar algunos, que requieren una estrategia de gestión de bots más amplia. Los requisitos clave de una solución de gestión de bots completa incluyen:

- tecnología de detección de bots dedicada que se adapte a unas amenazas cada vez más sofisticadas;
- las capacidades más recientes y avanzadas para seguir detectando bots a medida que evolucionan;
- compatibilidad con la nube para gestionar los picos de tráfico que, de otro modo, podrían saturar la infraestructura de inicio de sesión;
- algoritmos de detección de alta precisión para preservar las experiencias de los usuarios legítimos;
- protección contra bots para las páginas de inicio de sesión, así como para todo el sitio web;
- acciones avanzadas y condicionales que le permiten gestionar el tráfico de bots y no solo mitigarlo, e
- información útil sobre el tráfico de bots conforme se desarrollan nuevos métodos para evitar la detección.

INTEGRE LA GESTIÓN DE BOTS EN SU ESTRATEGIA DE SEGURIDAD

Para obtener una mayor visibilidad de las amenazas online, las herramientas de gestión de bots también deberían integrarse fácilmente en su estrategia de seguridad web general. Una solución de seguridad completa que incluya un WAF, protección contra ataques distribuidos de denegación de servicio (DDoS) y gestión de bots le ayudará a identificar mejor la verdadera naturaleza de las amenazas contra su sitio web.

Por ejemplo, un pico de tráfico que desmantele el servidor de inicio de sesión puede parecer, a primera vista, un ataque DDoS. Si solo cuenta con protección contra DDoS, detener el ataque puede dar la falsa impresión de que se ha mitigado el riesgo. Sin embargo, combinar la protección contra DDoS con la gestión de bots permite mantener la disponibilidad e identificar la causa raíz: un repunte en las solicitudes de inicio de sesión derivado del relleno de credenciales.

Además, las interfaces de usuario integradas para la protección contra DDoS, así como las soluciones WAF y de gestión de bots, le permiten ver la actividad sospechosa en las distintas aplicaciones. Asimismo, un único destino para incluir en la lista blanca los bots útiles, como los rastreadores de motores de búsqueda, le ayudará a gestionar la actividad online de manera más eficiente. En caso de que se produzca un evento de seguridad, puede acceder a una fuente centralizada para ver todos los vectores de ataque y agilizar la resolución.

OnTek

Obtenga más información sobre cómo gestionar y mitigar amenazas de bots como el relleno de credenciales en **www.ontek.net**

Póngase en contacto con nosotros para descubrir cómo las nuevas tecnologías avanzadas pueden mejorar su estrategia de seguridad online.